UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,331	10/14/2003	Richard M. Butler	10991268-3	7201

22879   7590   11/26/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
DO, CHAT C

ART UNIT	PAPER NUMBER
2193	

MAIL DATE	DELIVERY MODE
11/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/686,331	BUTLER, RICHARD M.
	Examiner	**Art Unit**	
	Chat C. Do	2193	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>22 August 2007</u>.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-22</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☒ Claim(s) <u>22</u> is/are allowed.

6) ☒ Claim(s) <u>1-3, 7-18, and 20-21</u> is/are rejected.

7) ☐ Claim(s) <u>4-6 and 19</u> is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This communication is responsive to Amendment filed 08/22/2007.

2. Claims 1-22 are pending in this application. Claims 1 and 22 are independent claims. In Amendment, claim 1 is amended. This Office Action is made final.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3, 7-18, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koopman Jr. (U.S. 5,757,923) in view of Nozuyama (U.S. 5,867,409).

Re claims 1-2, Koopman Jr. discloses in Figure 1 a method of generating a random number (e.g. output of component 40 as random digital data stream), comprising: sampling (e.g. by component 25 in Figure 1) data transmitted over a number of microprocessor buses (e.g. wherein the recording device 15 has a microprocessor for capturing the chaotic noise source from component 10) at input of a number of a processed component (e.g. processing component 35 for generating random numbers) coupled with the number of microprocessor buses (e.g. connecting with the components 25 and 15); generating values within the processed component based on the sampled data

(e.g. col. 6 lines 1-7); retrieve the values from the number of processed component (e.g. with corresponding memory array 30 in Figure 1); and generating a random number which is based on the values retrieved from the number of the processed component (e.g. output of component 40 as random digital data stream in Figure 1).

Koopman Jr. fails to disclose the processed component is multiple input shift registers (MISRs) and the number of MISRs is one. However, Nozuyama discloses in Figures 2-3 the processed component is MISR wherein the inputs are Dx and outputs are OUTx and the number of MISRs is one (e.g. Figures 2-3 as one MISR).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to replace the processed component with a multiple MISRs as one as disclosed in Nozuyama's Figure 2 into Edelkind et al.'s Figure 4 because it would enable to increase the randomness and performance of the system random output (e.g. col. 2 lines 6-46).

Re claim 3, Koopman Jr. further discloses in Figure 1 one of the number of MISRs is coupled to a data address bus which transfers data between a data cache and a CPU core (e.g. data cache is digitizer storage 25 and the microprocessor is the recording device 15 in Figure 1, thus the sampler is sampling data in between).

Re claim 7, Koopman Jr. further discloses in Figure 1 one of the number of MISRs is coupled to a bus which runs wholly within an integrated circuit package (e.g. Figure 1 as single package).

Re claim 8, Koopman Jr. fails to disclose in Figure 1 retrieving values from the number of MISRs comprises: loading bits of a value stored in a first of the number of

MISRs, in parallel, into a temporary register; and retrieving the value stored in the temporary register. However, Nozuyama discloses in Figures 3 and 7 retrieving values from the number of MISRs comprises: loading bits of a value stored in a first of the number of MISRs, in parallel, into a temporary register; and retrieving the value stored in the temporary register (e.g. Figures 3 and 7).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add step of retrieving values from the number of MISRs comprises: loading bits of a value stored in a first of the number of MISRs, in parallel, into a temporary register; and retrieving the value stored in the temporary register as seen in Nozuyama's invention into Koopman Jr.'s invention because it would enable to efficiently generate random number.

Re claim 9, Koopman Jr. fails to disclose in Figure 1 retrieving values from the number of MISRs comprises retrieving a value from a first of the number of MISRs by stepping the first of the number of MISRs to serially shift a plurality of bits out of the MISR. However, Nozuyama discloses in Figure 1 retrieving values from the number of MISRs comprises retrieving a value from a first of the number of MISRs by stepping the first of the number of MISRs to serially shift a plurality of bits out of the MISR (e.g. Figures 1 and 3)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to retrieve values from the number of MISRs comprises retrieving a value from a first of the number of MISRs by stepping the first of the number of MISRs to serially shift a plurality of bits out of the MISR as disclosed in Nozuyama's

Figure 1 into Edelkind et al.'s Figure 4 because it would enable to increase the

randomness of the system random output.

Re claim 10, Koopman Jr. further discloses in Figure 1 generating a random

number comprises hashing together the values retrieved from the number of MISRs (e.g.

by component 35 in Figure 1).

Re claim 11, Koopman Jr. further discloses in Figure 1 generating a random

number comprises XORing the values retrieved from the number of MISRs (e.g. by

component 35 in Figure 1 and col. 6 lines 1-6).

Re claim 12, Koopman Jr. in view of Nozuyama fails to disclose in Figure 1

turning on and initializing each of the number of MISRs upon boot of a computer in

which the MISRs reside. However, the examiner takes an official notice that these flip-

flops only hold the data when the power is on so the flip-flops will reset upon power

initialization.

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention is made to initialize the MISR upon the power reset because it

would enable to start a new sequence of random number.

Re claim 13, Koopman Jr. further discloses in Figure 1 values are retrieved from

the number of MISRs via an operating system call (e.g. by component 35 in Figure 1).

Re claim 14, Koopman Jr. further discloses in Figure 1 operating system call is of

a highest privilege level (e.g. by component 35 in Figure 1).

Re claim 15, Koopman Jr. further discloses in Figure 1 generating a random

number is performed immediately after the number of MISR readings are taken (e.g. by

component 35), the method further comprising storing the random number in a temporary location for subsequent use (e.g. component 42 as temporary memory).

Re claim 16, Koopman Jr. further discloses in Figure 1 operating system call is issued in response to an application's request for a random number (e.g. by component 35 in Figures 1-2 and 4).

Re claim 17, Koopman Jr. fails to disclose the retrieved values from a number of MISRs comprises a computer program's issuance of a request to read the number of MISRs. However, Nozugama discloses that the retrieved values from a number of MISRs comprises a computer program's issuance of a request to read the number of MISRs (col. 1 lines 35-40).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add a program's issuance as disclosed in Nozugama into Edelking et al.'s invention because it would enable to test the output of the random system prior outputting.

Re claim 18, Koopman Jr. further discloses in Figure 1 generating said random number comprises providing the values retrieved from the number of MISRs, as well as historic values retrieved from the number of MISRs, to a pseudo-random number generator (e.g. by component 35 in Figure 1 wherein the MIRS as the processed component).

Re claim 20, Koopman Jr. further discloses in Figure 1 the random number is an encryption key (e.g. Figure 4).

Re claim 21, Koopman Jr. fails to disclose in Figure 1 the MISRs form part of a microprocessor's built-in self-test hardware. However, Nozuyama discloses in Figure 7 the MISRs form part of a microprocessor's built-in self-test hardware (e.g. col. 9 lines 27-68).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention is made to add the MISRs form part of a microprocessor's built-in self-test hardware as seen in Nozuyama's invention into Koopman Jr.'s invention because it would enable to improve the performance (e.g. col. 3 lines 21-36).

Allowable Subject Matter

5.   Claim 22 is allowed.

6.   Claims 4-6 and 19 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

7.   Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

8.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

        A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

        Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Chat C. Do whose telephone number is (571) 272-3721. The

examiner can normally be reached on M => F from 7:00 AM to 5:30 PM.

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Meng-Ai An can be reached on (571) 272-3756. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

<div style="text-align:right">

Chat C. Do
Examiner
Art Unit 2193

</div>

November 19, 2007